

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-202129

(43)Date of publication of application : 27.07.2001

(51)Int.Cl.

G05B 23/02
F02D 45/00
G06F 11/10
G06F 12/16
// B60R 16/02
B60S 5/00

(21)Application number : 2000-012802

(71)Applicant : DENSO CORP.

(22)Date of filing : 21.01.2000

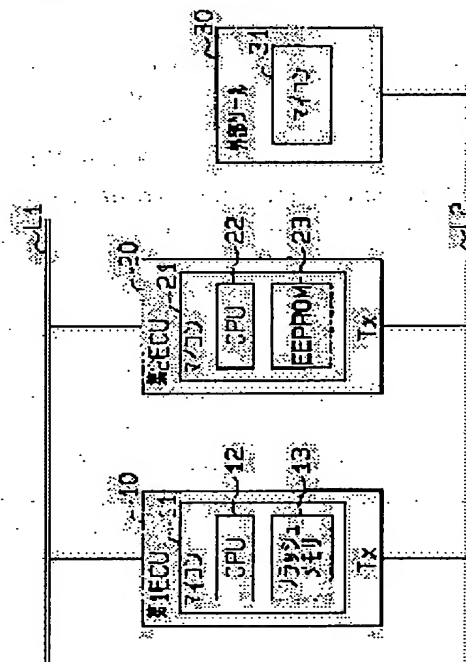
(72)Inventor : NAKAYAMA KIYONARI
KAMIYA KENJI

(54) METHOD FOR INSPECTING ON-VEHICLE CONTROL UNIT

(57)Abstract:

PROBLEM TO BE SOLVED: To correctly inspect an on-vehicle control unit and to prevent the unit from being illegally modified.

SOLUTION: First and second ECUs 10, 20 are mutually connected so as to be communicated with each other through a multiplex communication line L1 and an external tool 30 is connected to respective ECUs 10, 20 through a serial communication line L2. In the decision of (inspecting) the corresponding/ falseness of the 1st ECU 10, the external tool 30 sends transmission data including a sum value calculation command to respective ECUs 10, 20 through the line L2. The 1st ECU 10 receives the sum value calculation command, calculates the sum value of data stored in a flash memory 13 and transmits the sum value to the 2nd ECU 20 through the line L1. The 2nd ECU 20 compares and decides the received sum value with a true sum value and transmits the decided result to the tool 30 through the line L2. Whether the 1st ECU 10 is a normal ECU or a false ECU is decided on the basis of the decision result.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-202129

(P2001-202129A)

(43) 公開日 平成13年7月27日 (2001.7.27)

識別記号	PI	チャート(参考)
G05B 23/02	302	302K 3D026
F02D 45/00	376	376F 3G084
G06F 11/10	310	310B 5B001
320	12/18	320B 5B018
B60R 16/02	665	665P 5H223

審査請求 未請求 願事項の款7 OL (全9頁) 最終頁に添く

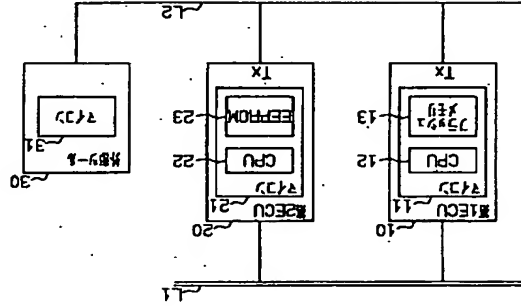
(21) 出願番号	特願2000-128021 (P2000-128021)	(71) 出願人	000004250 株式会社デンソー
(22) 出願日	平成12年1月21日 (2000.1.21)	(72) 発明者	株式会社デンソー 愛知県刈谷市昭和町1丁目1番地 株式会社 中山 理也 社デンソー内 神谷 敏治 愛知県刈谷市昭和町1丁目1番地 株式会社 社デンソー内 愛知県刈谷市昭和町1丁目1番地 株式会社 社デンソー内 (74) 代理人 10006755 弁護士 尾田 博彦 (外1名)

(56) 【発明の名称】 車載制御ユニットの検査方法

(57) 【要約】

【課題】 車載制御ユニットを正しく検査し、ひいては不正改造の防止を図る。

【解決手段】 第1及び第2 ECU 10、20は多量通信線L1を介して相互に通信可能に接続され、外部ツール30はシリアル通信線L2を介して各 ECU 10、20に接続されている。第1 ECU 10の正値判定(検査)に際し、外部ツール30では、サム値の算出指令を含む送信データをシリアル通信線L2を介して各 ECU 10、20に送信する。第1 ECU 10では、サム値算出指令を受け、そのサム値を多量通信線L1を介して第2 ECU 20に送信する。第2 ECU 20では、受信したサム値と真のサム値とを比較判定し、その判定結果をシリアル通信線L2を介して外部ツール30に送信する。この判定結果により、第1 ECU 10が正規 ECUか偽 ECUかが判断される。



(2)

特開平13-202129

【特許請求の範囲】

【請求項1】 チェックサムの対象となるメモリを備える第1の制御ユニットと、それとは別の第2の制御ユニットとを備え、前記第1の制御ユニットのメモリについてデータのサム値を求め、該サム値により当該第1の制御ユニットを検査する車載制御ユニットの検査方法において、

サム値の算出指令を外部ツールから第1の制御ユニットへ送信する第1のステップと、

第1の制御ユニット内のメモリのサム値を算出し、該算出したサム値を第2の制御ユニットに送信する第2のステップと、

第2の制御ユニットにおいて受信したサム値を予め用意された真のサム値と比較し、その比較判定の結果から第1の制御ユニットを検査する第3のステップと、

前記検査結果を外部ツールに送信する第4のステップと、

からなることを特徴とする車載制御ユニットの検査方法。

【請求項2】 第1の制御ユニット内のメモリは、電気的に書き換え可能な不揮発性メモリである請求項1に記載の車載制御ユニットの検査方法。

【請求項3】 前記第2のステップでは、外部ツールが検査される通信線とは異なる別の通信経路を用いて、第1の制御ユニットから第2の制御ユニットへサム値を送信する請求項1又は2に記載の車載制御ユニットの検査方法。

【請求項4】 外部ツールは、サム値算出指令の送信後、所定の応答待ち時間以内に受信した受信データを無効とする請求項1～3の何れかに記載の車載制御ユニットの検査方法。

【請求項5】 第2の制御ユニットは、外部ツールがサム値算出指令を送信した後、所定の制限時間以内に第1の制御ユニットからサム値が送信されない場合、当該第1の制御ユニットが不正である旨のコード情報を自身の不揮発性メモリに書き込む請求項1～3の何れかに記載の車載制御ユニットの検査方法。

【請求項6】 第1の制御ユニットが不正である旨が判定された状態で、第1の制御ユニットから外部ツールへのデータ送信が行われる場合、第2の制御ユニットは、第1の制御ユニットと外部ツールとを結ぶ通信線にダミーデータを送出する請求項1～3の何れかに記載の車載制御ユニットの検査方法。

【請求項7】 請求項6に記載の車載制御ユニットの検査方法において、

第2の制御ユニットは、データの送信ポートを論理レベル又はローレベルに保持することでダミーデータを送出する車載制御ユニットの検査方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、車載制御ユニットの検査方法に関するものである。

【0002】

【従来の技術】 この種の従来技術として、特開平11-132097号公報の「車載制御用メモリ書き換え装置」がある。同公報の装置は、外部ツールにより電気的に消去及び書き込み可能な制御メモリ(フラッシュメモリ)を搭載した ECU (車載制御ユニット) を備え、書き換え許可された時にのみ前記制御メモリに対するデータ書き換えが実施される。また、この装置は、制御メモリが記憶するソフトウェア(制御プログラム)が正しいことを検査するものであり、その特徴として、

・予め記憶しておいた制御メモリのサム値(真値)と、ECUで算出したサム値とを共に表示し、それらと比較することで正偽判定を行う。

・上記サム値の比較は外部ツールの内部で行い、その結果(正偽)のみを返す。

・イグニッションキースイッチのOFFからONへの切換え後にサム値の計算を行う、といった処理を実行する。

【0003】

【発明が解決しようとする課題】 上記公報の従来技術では、ECUで計算したサム値を外部ツールに対してそのまま送信する。そのため、ECUと外部ツールとの通信データをモニタすることにより、ECUにより算出した正しいサム値を容易に知り得ることができ、

【0004】 また、制御メモリのサム値は、ソフトウェアを書き換えなければならないものであるため、外部ツールに対して正しいサム値を常に送信するような不正なプログラムを不正改造者が作成し、それをECUに組み込めば、正規のサム値算出アルゴリズムを知らなくとも容易に正規 ECU としてなり得ることが可能となる。これは、ECU側で正偽判定を行う構成でも同様である。すなわち、モニタしたサム値を返答する偽プログラムを不正改造者が作成することにより、不正改造された偽 ECU であっても、外部ツールは正しいサム値(真値に同じ)が返答されたと認識し、正しい ECU であると判断してしまう。

【0005】 本発明は、上記問題に著目してなされたものであって、その目的とするところは、車載制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる車載制御ユニットの検査方法を提供することにある。

【0006】

【課題を解決するための手段】 請求項1に記載の車載制御ユニットの検査方法は、(1) サム値の算出指令を外部ツールから第1の制御ユニットへ送信する第1のステップ、(2) 第1の制御ユニット内のメモリのサム値を算出し、該サム値を第2の制御ユニットに送信する第2のステップ、(3) 第2の制御ユニットにおいて受信したサム値を予め用意された真のサム値と比較

し、その比較判定の結果から第1の制御ユニットを検査する第3のステップ、(4) 前記検査結果を外部ツールに送信する第4のステップ、といった各ステップを順に実施する。そのため、仮に正規の制御ユニットが不正改造され、メモリの正しい値を外部ツール側に送信できるような不正なプログラムが制御ユニットに組み込まれたとしても、第2の制御ユニットの改造又は置換を併せて実施しなければ、偽の制御ユニットが正規の制御ユニットとしてなりすますことはできない、その結果、単独制御ユニットを正しく検査し、ひいては不正改造の防止を図ることができる。

【0007】上記説明は特に、フラッシュメモリ等、電気的に書き換え可能な不揮発性メモリにて第1の制御ユニット内のメモリが構成される場合に有効である（請求項2）。

【0008】請求項3に記載の発明では、前記第2のステップにおいて、外部ツールが接続される通信線とは異なる別の通信線を用いて、第1の制御ユニットから第2の制御ユニットへサム値を送信する。本発明によれば、第1の制御ユニットから発信されるサム値の発信結果が外部ツールで受信されることがないので、外部ツール側で本来受けないデータが受信され、それが原因で処理が滞るといった不都合が回避される。

【0009】請求項4に記載の発明では、外部ツールは、サム値送信指令の送信後、所定の応答待ち時間以内に受信した受信データを無効とする。つまり、外部ツールがサム値算出指令を送信すると、当該外部ツールは本来、上記第2～第4の各ステップが実施される処理時間を越えた後、サム値算出指令に応答するデータを受信する。こうした状況にもかかわらず、サム値算出指令の後、直ぐに外部ツールがデータを受信した場合、制御ユニットが不正改造された可能性が高い。そのため、規定に満たない時間で受信したデータを無効化すると共に、制御ユニットが不正改造された旨を判断する。

【0010】請求項5に記載の発明では、第2の制御ユニットは、外部ツールがサム値算出指令を送信した後、所定の制限時間以内に第1の制御ユニットからサム値が送信されない場合、当該第1の制御ユニットが不正である旨のコード情報自身（第2の制御ユニット内）の不揮発性メモリに書き込む。かかる場合にも、制御ユニットが不正改造されたことが判定でき、更にその旨を不揮発性メモリに格納することにより、後々の異常診断に役立てることができる。なお、不揮発性メモリに書き込まれたコード情報は、外部ツールからの要求に従い、第2の制御ユニットから外部ツールに送信される。良い。

【0011】ところで、第2の制御ユニットにより第1の制御ユニットを検査し、その結果を外部ツールに送信する上記構成では、第1の制御ユニットが不正改造されていても、不正改造された当の制御ユニットが自身を正確なECUであるとするデータを送信すると、外部ツール

は不正改造された制御ユニットを正規なものとして判断するおそれがある。

【0012】そこで、請求項6に記載の発明では、第1の制御ユニットが不正である旨が判定された状態で、第1の制御ユニットから外部ツールへのデータ送信が行われる場合、第2の制御ユニットは、第1の制御ユニットと外部ツールとを結ぶ通信線にダイナミックデータを送出する。これにより、不正改造された制御ユニットから外部ツールへ向けられたデータが送出したとしても、ダイナミックデータで前記データが破壊（無効化）される。従って、不正改造された制御ユニットを外部ツールが正規なものとして判断するといった不都合が解消される。

【0013】特に、請求項7に記載したように、第2の制御ユニットは、データの送信ポートを管理ハイレベル又はローレベルに保持することでダイナミックデータを送出すると共に、これにより通信線構成での実現が可能となる。

【0014】**【発明の実施の形態】**（第1の実施の形態）この発明を具体化した本実施の形態では、エンジン制御等を行うECUにて車載制御ユニットを構成しており、このECUに対して外部ツールを接続し、当該ECUの検査やデータの交換等を行うこととしている。以下、その詳細を図面に従って説明する。

【0015】図1は、制御システム全体の構成を示すブロック図である。本システムでは、第1の制御ユニットとしての第1ECU10と、第2の制御ユニットとしての第2ECU20とを備える。これらの第1及び第2ECU10、20は、多量通信線L1を介して相互に通信可能に接続されている。第1ECU10は、燃料噴射制御や点火時期制御等、エンジン内の主要な制御を受け持つECUであり、その内部のマイコン11は、各種制御の中枢をなすCPU12、電気駆動時にも記憶内容を保持するEEPROM23、その他図示しないRAMや出力回路等を備える。

【0016】また、第2ECU20は、エアバグ制御やABS制御等、補助的な制御を受け持つECUであり、その内部のマイコン21は、各種制御の中枢をなすCPU22、電源駆動時にも記憶内容を保持するEEPROM23、その他図示しないRAMや出力回路等を備える。

【0017】外部ツール30も同様に、CPU、メモリ、入出力回路等からなる周知のマイコン31を備える。この外部ツール30は、第1ECU10の正値判定等の検査や、第2ECU10内のフラッシュメモリ13のデータ書き換えに際し、シリアル通信線L2を介して第1及び第2ECU10、20と接続される。これにより、第1及び第2ECU10、20と外部ツール30との間でシリアル通信によるデータのやり取りが行われる。

【0018】第1ECU10の正値判定（検査）の概要

を、図2を用いて説明する。かかる場合、フラッシュメモリ13内のデータのサム値と既知の正しいサム値と比較され、両者が一致すれば、第1ECU10が正規なものであると判断される。なお図2では、処理順序を致すため、(1)～(5)の連続番号を付けている。

【0019】先ず始めに、サム値の算出指令を含む送信データをシリアル通信線L2を介して外部ツール30から各ECU10、20に送信する（図の(1)）。第1ECU10側では、サム値算出指令を受け持つフラッシュメモリ13内のデータのサム値Xsumを算出し（図の(2)）、その後、そのサム値Xsumを多量通信線L1を介して、すなわち外部ツール30が接続されるシリアル通信線L2とは異なる別の通信線を通じて、第2ECU20に送信する（図の(3)）。

【0020】第2ECU20では、受信したサム値Xsumと、予め登録されている真のサム値Xrefとを比較判定し、その判定結果をシリアル通信線L2を介して外部ツール30に送信する（図の(4)）。また、この第2ECU20では、サム値不一致の場合に第1ECU10が不正改造されたことを検知するダイナミックデータを記述する。

【0021】そして、前記判定結果がサム値の一致（Xsum=Xref）を表すものである場合は、外部ツール30において第1ECU10が正規ECUであると判断し、前記判定結果がサム値の不一致（Xsum≠Xref）を表すものである場合は、外部ツール30において第1ECU10が偽ECUであると判断する。

【0022】以下では、外部ツール30による第1ECU10の正値判定に際し、各ECU10、20及び外部ツール30内の各マイコン11、21、31により実施される処理の流れを図3及び図4のフローチャートに依り説明する。始めに、外部ツール30の処理の流れを図3のフローチャートで説明する。

【0023】例えば修理工場等において作業者が外部ツール30を操作することで図3の処理がスタートし、先ずステップ101では、コマンド送信処理によりサム値算出指令を各ECU10、20に送信する。また、ステップ102ではダイナミックデータを送信する。このステップ101、102が通信前処理に相当する。

【0024】その後、この外部ツール30では、コマンド送信に対する第2ECU20からの受信処理を行う。すなわち、タイムアウトしないことを条件に（ステップ103がNO）、ステップ104では、前記ステップ100のコマンド送信に対する応答を第2ECU20から受信したか否かを判断する。

【0025】応答が無いままタイムアウトした場合（ステップ103がYES）、そのままステップ107に進む。ステップ107では、通信異常に際するダイナミックデータを取り出し、その後、ECU異常の旨を判断する。なお、ステップ103がYESの場合、ステップ101

に戻り、コマンド送信を再度実施しても良い。この場合、コマンド再送信の回数を予め制限しておき、例えばタイムアウトが3回繰り返されるまで、通信異常であると判断してステップ107に進む構成しても良い。

【0026】コマンド送信に対する応答を第2ECU20から受信すると、ステップ105に進み、その受信データ内に含まれるサム値の判定結果を取り出す。そして、その判定結果がサム値一致に該当するものである場合は、ステップ106を肯定判断し、ECU正常である旨を判断する。また、前記判定結果がサム値不一致に該当するものである場合は、ステップ108を肯定判断し、ステップ107でダイナミックデータを取り出し、その後、ECU異常の旨を判断する。

【0027】次に、第1及び第2ECU10、20の処理の流れを図4のフローチャートに依り説明する。ここで、図4(a)は第1ECU側10の処理を示し、図4(b)は第2ECU20側の処理を示す。先ず、図4(a)に依り、第1ECU10側の処理の流れを説明する。

【0028】第1ECU10内のマイコン11は、先ずステップ201において、外部ツール30よりコマンドを受信したか否かを判断し、YESであればステップ202に進み、算出式 $Xsum = \sum Data(i)$ により、サム値Xsumを算出する。すなわち、フラッシュメモリ13内の規定されたアドレス領域についてアドレスのデータを全て加算し、その和をサム値Xsumとする。その後、ステップ203では、前記算出したサム値Xsumを多量通信線L1を介して第2ECU20に送信し、本処理を一旦終了する。

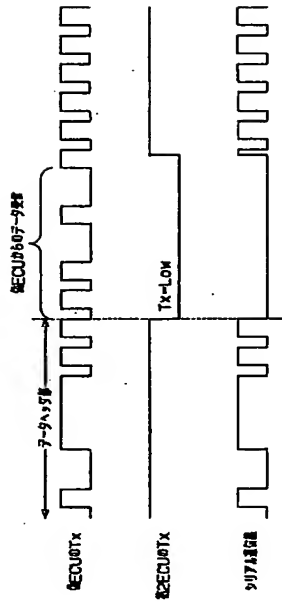
【0029】一方、第2ECU20内のマイコン21は、図4(b)のステップ301において、第1ECU10よりサム値Xsumを含むデータを受信したか否かを判断し、YESであればステップ302に進み、受信データからサム値Xsum（生データ）を取り出す。

【0030】その後、ステップ303では、予め登録されている真のサム値Xrefを取り出し、算出したステップ304では、サム値Xsum（生データ）と真のサム値Xrefとを比較する。

【0031】両サム値が一致すれば、そのままステップ308に進み、サム値の比較結果をシリアル通信線L2を介して外部ツール30に対して送信する。この場合、前記図3の処理では、ECU正常である旨が判断される。

【0032】また、両サム値が不一致であれば、ステップ305で第1ECU10が不正改造されたことを意味するダイナミックデータをEEPROM23に登録した後、ステップ306でデータの比較結果をシリアル通信線L2を介して外部ツール30に対して送信する。この場合、外部ツール30による前記図3の処理では、EEP

【図9】



フロントページの続き

(51)Int.Cl. ⁷ B60S 5/00	特許庁長官 B60S 5/00	FI B60S 5/00	特許庁長官 9A001
---------------------------------------	--------------------	-----------------	----------------

Fターム(参考) 3D025 B422 B428
3G084 B400 D432 B806 B822
5B001 A414 A801 A001 A003 A201
5B018 G403 G406 G410 H413 H431
J426 K412 N406 B411 B412
5H223 A410 C008 D003 E211 E219
9A001 B803 H234 J777 L406

THIS PAGE BLANK (USPTO)